Heroes Academy

Securing WebAPI calls with JWT

Peter Rombouts
Senior Technologiespecialist Microsoft

Vianen, 25 Januari 2017

peter.rombouts@sogeti.com
microsofthelden.nl

Agenda

1. Wat is een JSON Web Token?
2. Tokens en Security
3. Demo
4. Authentication Scenarios for Azure AD
5. Demo
6. Aandachtspunten

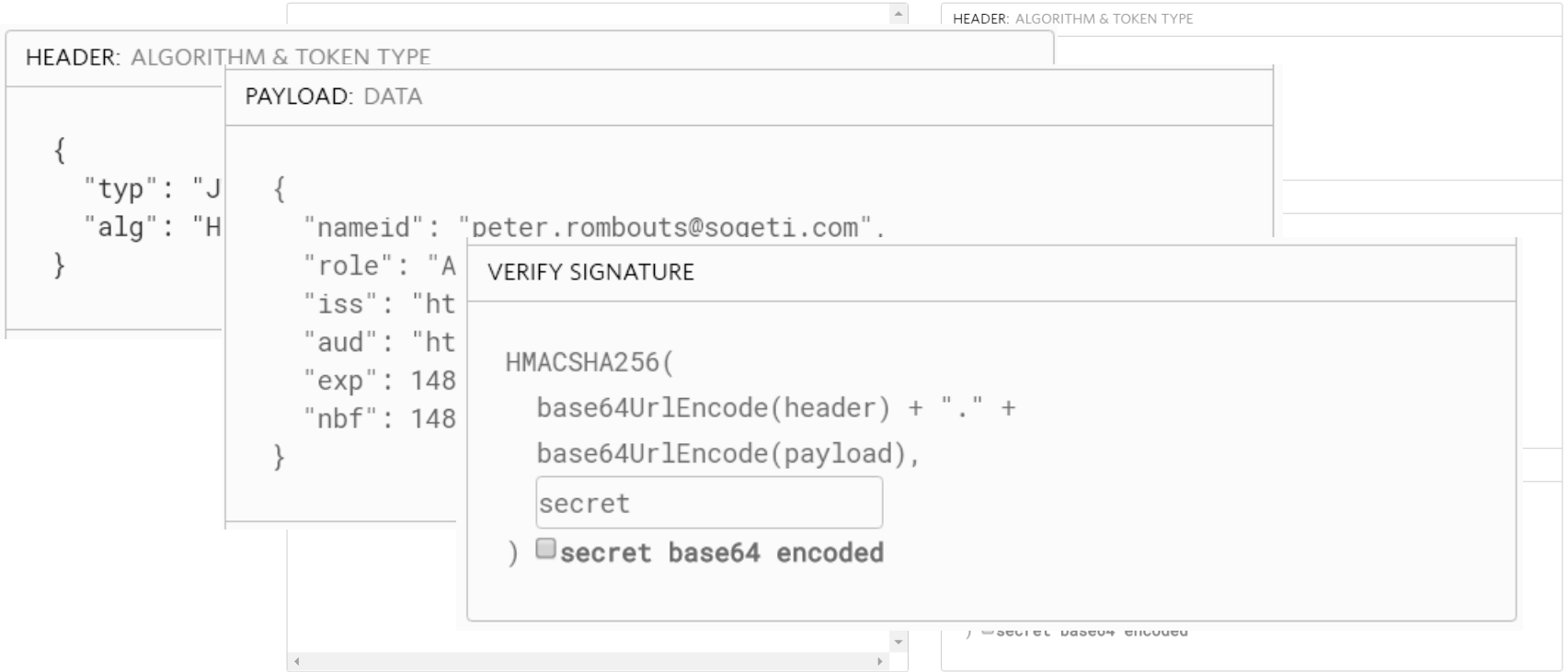
Wat is een JSON Web Token?

“JSON Web Tokens are an open, industry standard RFC 7519 method for representing claims securely between two parties.”

Bestaat uit

- **Header**
- **Payload (Claims)**
- **Signature**

Wat is een JSON Web Token?



Tokens en Security

Informatiebeveiliging in stappen

1. **Identificatie**
   Het kenbaar maken van de identiteit van een subject (een gebruiker/proces)

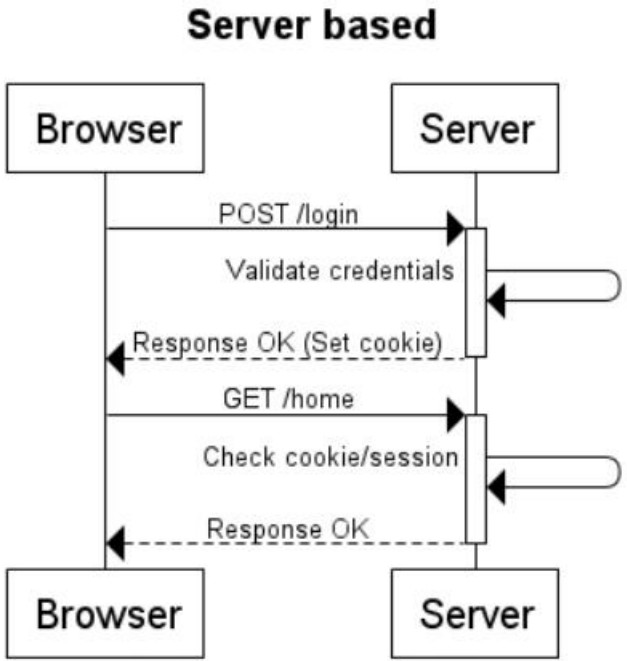
2. **Authenticatie**
   Het proces waarbij iemand nagaat of een gebruiker, een andere computer of applicatie daadwerkelijk is wie hij beweert te zijn.

3. **Autorisatie**
   Het proces waarin een subject (een persoon of een proces) rechten krijgt op het benaderen van een object (een bestand, een systeem).

Tokens en Security

Server gebaseerd

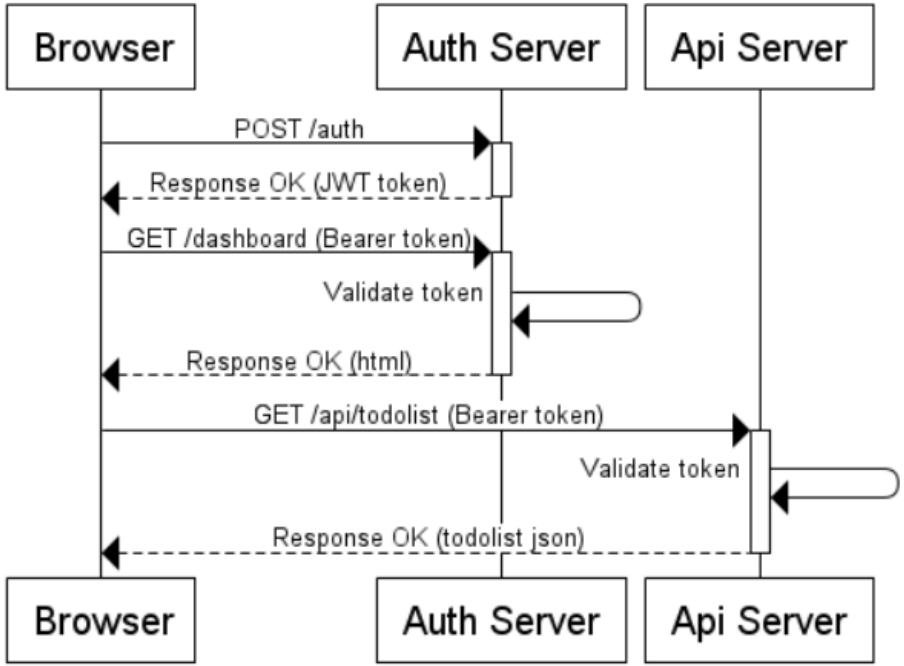
- **Stateful**
- **Lastig schaalbaar**
- **Performance (serialisatie/deserialisatie)**
- **Platform afhankelijk**



Tokens en Security

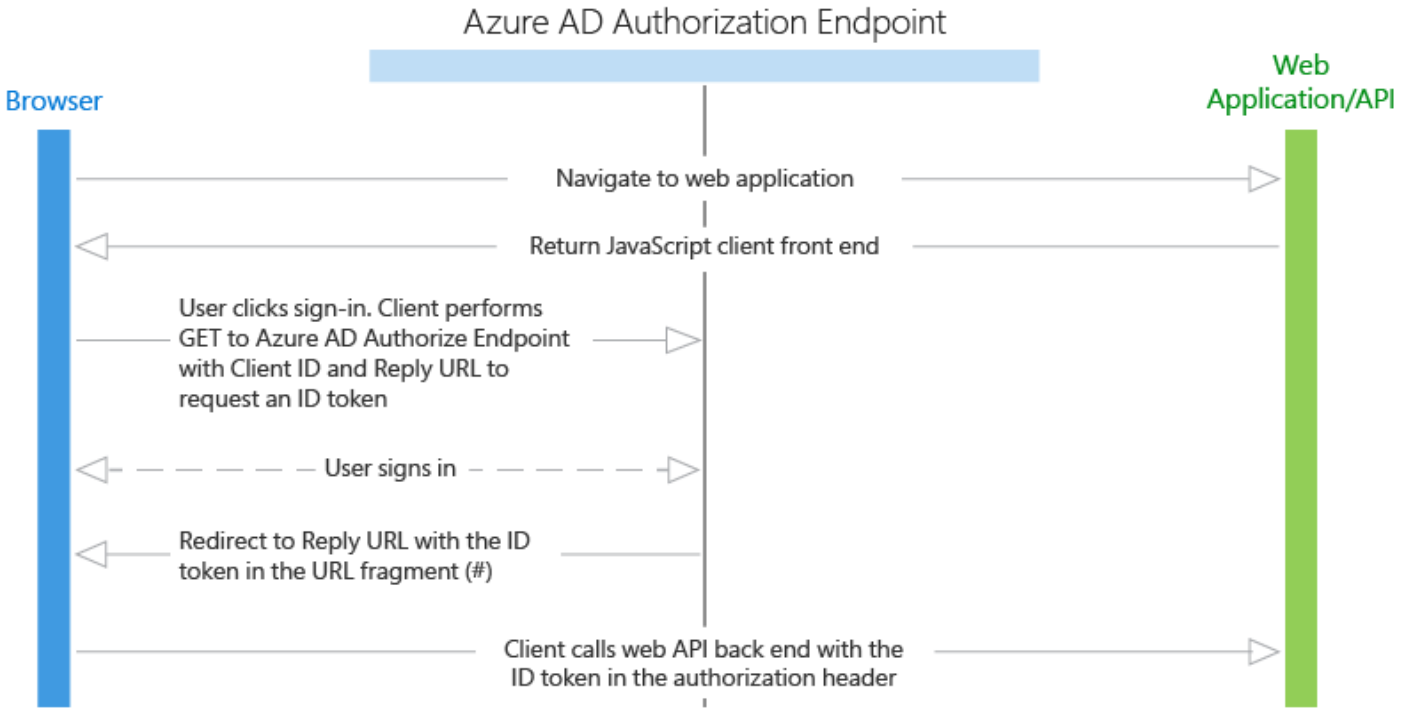
Token gebaseerd

- **Stateless**
- **Schaalbaar**
- **Performance**
- **Platform onafhankelijk**



Demo

Azure AD


Azure AD Authorization Endpoint
Browser
Web Application/API
Navigate to web application
Return JavaScript client front end
User clicks sign-in. Client performs GET to Azure AD Authorize Endpoint with Client ID and Reply URL to request an ID token
User signs in
Redirect to Reply URL with the ID token in the URL fragment (#)
Client calls web API back end with the ID token in the authorization header

Demo

Active Directory Authentication Library for JavaScript (ADALJS)

Aandachtspunten

JWT is een authenticatie protocol, geen framework zoals OAuth2

- **Tokens hebben een grootte limiet**
- **Tokens kunnen niet worden ingetrokken (revocation)**
- **Zorg daarom voor een korte levensduur (expiration)**

Security is veel meer! Denk bijvoorbeeld aan

- **Secure Coding / Ethical Hacking / Audits**
- **Database Security / SIEM / Firewalling / Network Infrastructure**

Links en meer

Links en Info:

- **JWT** https://jwt.io/
- **OAuth2** https://oauth.net/2/
- **Postman** https://www.getpostman.com/
- **Active Directory Authentication Library for JavaScript**
  https://github.com/AzureAD/azure-activedirectory-library-for-js
- **Authentication Scenarios for Azure AD (SPA)**
  https://docs.microsoft.com/en-us/azure/active-directory/develop/active-directory-authentication-scenarios#single-page-application-spa

Packages:

- **Angular JWT:** https://github.com/auth0/angular-jwt
- **System.IdentityModel.Tokens.Jwt** http://www.nuget.org/packages/System.IdentityModel.Tokens.Jwt/